

POLÍTICA DE GOBERNANZA DE DATOS

1. OBJETIVO

La presente Política de Gobernanza de Datos (la **“Política”**) tiene por objeto establecer el marco regional que orienta la gestión, uso, protección, seguridad, calidad y disponibilidad de los datos tratados por **Emergent Cold LatAm (“Emergent Cold”, “ECLA” o la Compañía)**, asegurando que su administración se realice de manera lícita, segura, responsable y alineada con los objetivos estratégicos del negocio y la continuidad operativa.

Esta Política define los lineamientos corporativos para la gobernanza de datos en todas las operaciones de la región, promoviendo prácticas consistentes que permitan gestionar los datos como un activo estratégico, reducir riesgos asociados a su tratamiento, fortalecer la confiabilidad de la información y garantizar el cumplimiento de la legislación vigente en cada país en materia de privacidad, protección de datos personales, seguridad de la información y normas sectoriales relacionadas.

Asimismo, esta Política establece la estructura regional y local para la supervisión, coordinación y escalamiento en materia de gobernanza de datos, incluyendo los roles y responsabilidades aplicables a las funciones de supervisión y control, tales como los equipos de Compliance, Tecnología, Seguridad de la Información y otros actores relevantes. Su propósito es asegurar una adecuada separación de funciones, independencia operativa en los roles de supervisión y una coordinación efectiva con los responsables locales del tratamiento de datos.

La implementación de esta Política permite a Emergent Cold LatAm consolidar un modelo regional de gobernanza integral, basado en principios de calidad, trazabilidad, transparencia, minimización de riesgos y mejora continua a lo largo del ciclo de vida del dato.

2. ALCANCE

Estos lineamientos tienen aplicabilidad para lo siguiente:

- a. Todos los datos generados, recibidos, administrados, almacenados o utilizados por Emergent Cold LatAm, cualquiera sea su soporte (físico, digital o mixto) y su naturaleza. Esto incluye, de manera no limitativa, datos operacionales,

comerciales, contractuales, logísticos, administrativos, financieros, de continuidad operativa, de seguridad de la información y cualquier otro dato necesario para las actividades de la Compañía. Asimismo, se incluyen todos los datos personales y, cuando corresponda, datos sensibles o de categoría especial tratados en el marco de las operaciones.

- b. Todos los tratamientos de datos realizados en el contexto de las actividades de Emergent Cold LatAm, incluyendo —a modo ejemplificativo— datos de contacto de clientes (B2B), destinatarios, remitentes, proveedores, transportistas, visitantes, colaboradores, postulantes y cualquier otro tercero cuyos datos sean tratados por la Compañía.
- c. Todo el personal, cualquiera sea su régimen de vinculación contractual (empleados, contratistas, consultores, temporales), así como proveedores, encargados y subencargados que accedan, gestionen o traten datos por cuenta de la Compañía en cualquiera de los países donde opera.

Este alcance incluye todas las instalaciones, sistemas, procesos, unidades de negocio y operaciones tecnológicas que intervengan en el ciclo de vida de los datos, tanto en ambientes propios como en aquellos gestionados por terceros.

3. MARCO NORMATIVO

Esta Política se dicta e interpreta de conformidad con el marco legal vigente en cada uno de los países donde Emergent Cold LatAm desarrolla sus operaciones, incluyendo la normativa aplicable en materia de gobernanza de datos, protección de datos personales, seguridad de la información, ciberseguridad y continuidad operativa, según corresponda a la actividad de la Compañía.

Asimismo, se sustenta en las obligaciones regulatorias sectoriales y en las disposiciones emitidas por autoridades competentes a nivel regional, cuando estas impongan requisitos específicos para el tratamiento, resguardo, administración o protección de datos en el contexto de las actividades regulares.

ECLA adopta también principios, buenas prácticas y lineamientos internacionalmente reconocidos en materia de gobernanza de datos, gestión de riesgos, seguridad de la información y ciberseguridad, aplicándolos de manera proporcional y coherente con su modelo operativo y con la legislación aplicable en cada jurisdicción.

Finalmente, se integra con las políticas, procedimientos y lineamientos corporativos internos de Emergent Cold LatAm relacionados con la protección de datos personales, seguridad de la información, gestión de incidentes, continuidad del negocio y otros componentes del sistema regional de cumplimiento y gestión de riesgos, los cuales deben ser observados de manera complementaria.

4. DEFINICIONES

Para los efectos de esta Política, y sin perjuicio de las definiciones contenidas en la legislación aplicable en cada país, se entenderá por:

- **Gobernanza de datos:** Conjunto de estructuras, roles, principios, políticas, prácticas y procedimientos que orientan la gestión, uso, calidad, protección y administración de los datos durante todo su ciclo de vida, asegurando su aprovechamiento responsable y alineado a los objetivos corporativos.
- **Comité de Gobernanza de Datos (CGD):** Órgano responsable de liderar, supervisar y dar dirección estratégica a los lineamientos, iniciativas y controles asociados a la gobernanza de datos dentro de Emergent Cold LatAm.
- **Derechos de los titulares:** Facultades reconocidas por la normativa aplicable a las personas cuyos datos son tratados, las cuales pueden incluir acceso, rectificación, actualización, cancelación, oposición, bloqueo, portabilidad y cualquier otra prevista por la legislación vigente.
- **Procedimiento de ejercicio de derechos:** Procesos y canales internos habilitados por ECLA para recibir, gestionar y responder solicitudes de titulares dentro de los plazos y condiciones establecidos por la legislación aplicable y las políticas corporativas.
- **Responsable local de protección de datos:** Rol designado en cada operación local para coordinar la implementación de políticas de gobernanza de datos y protección de datos personales, gestionar riesgos, atender solicitudes de titulares y actuar como punto de enlace con el equipo regional.
- **Función Regional de Gobernanza y Protección de Datos:** Equipo o rol encargado de establecer lineamientos regionales, supervisar la implementación en cada país, dar soporte técnico y normativo, monitorear el cumplimiento y escalar incidencias o riesgos relevantes.
- **Dato o activo de información:** Cualquier información generada, recibida, administrada o utilizada, independientemente de su formato o soporte, y que posea valor operativo, legal, comercial o estratégico.

- **Calidad de datos:** Grado en que los datos cumplen atributos esenciales como exactitud, completitud, coherencia, vigencia y oportunidad, permitiendo decisiones y operaciones confiables.
- **Ciclo de vida del dato:** Conjunto de etapas que atraviesa un dato desde su creación o recolección, almacenamiento, uso, intercambio, actualización, archivo y finalmente su eliminación segura o anonimización.
- **Propietario de datos (Data Owner):** Rol o área responsable de definir el propósito, los criterios de calidad, los niveles de acceso y los requisitos de protección para un conjunto específico de datos.
- **Custodio o administrador de datos (Data Steward / Data Custodian):** Responsable de aplicar, mantener y monitorear los controles operativos necesarios para preservar la integridad, disponibilidad, calidad y trazabilidad de los datos en los sistemas bajo su administración.
- **Inventario de datos:** Registro estructurado que documenta los tipos de datos tratados por la Compañía, su ubicación, responsables, finalidades, flujos, niveles de criticidad y controles aplicables.
- **Clasificación de datos:** Proceso mediante el cual los datos se categorizan con base en su nivel de sensibilidad, criticidad o confidencialidad, estableciendo los requisitos de protección asociados.
- **Datos críticos:** Datos cuya pérdida, alteración, divulgación o indisponibilidad puede afectar de forma significativa la operación, la continuidad del negocio, el cumplimiento regulatorio, la seguridad o las relaciones comerciales de Emergent Cold LatAm.
- **Flujos de datos:** Movimientos o transferencias de datos entre sistemas, áreas, procesos, países o terceros, incluyendo intercambios internos y transmisiones externas.
- **Acceso autorizado:** Permiso otorgado a personas o sistemas, basado en principios de necesidad y proporcionalidad, para consultar, modificar o utilizar datos según las funciones asignadas.
- **Incidente de datos:** Cualquier evento que afecte o pueda afectar la integridad, confidencialidad, disponibilidad, calidad o trazabilidad de los datos, incluyendo accesos no autorizados, pérdida, destrucción, alteración o divulgación indebida.
- **Trazabilidad de datos:** Capacidad de conocer y reconstruir el origen, uso, modificaciones, accesos y movimientos de los datos a lo largo de su ciclo de vida.
- **Anonimización:** Proceso mediante el cual se eliminan los identificadores de un dato personal de manera irreversible, de modo que no sea posible asociarlo a una persona.

- **Seudonimización:** Técnica que reemplaza identificadores personales por códigos o atributos indirectos, reduciendo el nivel de exposición del dato sin impedir su utilización para ciertos fines permitidos.
- **Ecosistema de datos:** Conjunto de procesos, sistemas, plataformas, personas, tecnologías y reglas que interactúan para permitir la gestión, protección y uso de los datos dentro de Emergent Cold LatAm.

5. PRINCIPIOS RECTORES

La gobernanza de datos de Emergent se regirá, al menos, por:

- a. Licitud: todo tratamiento debe tener base de licitud determinada.
- b. Finalidad y compatibilidad: uso para fines explícitos y legítimos, evitando usos incompatibles.
- c. Minimización y proporcionalidad: solo datos estrictamente necesarios.
- d. Calidad e integridad: datos exactos, consistentes y actualizados.
- e. Confidencialidad y seguridad: medidas técnicas y organizativas adecuadas.
- f. Limitación temporal: conservación solo por el tiempo necesario; eliminación/anonimización oportuna.
- g. Transparencia: información clara a titulares cuando corresponda.
- h. Responsabilidad proactiva (accountability): evidencia documental del cumplimiento.
- i. Gestión basada en riesgos: controles proporcionales al riesgo del tratamiento (tipo de dato, volumen, exposición, criticidad operativa, terceros, tecnologías).

6. ROLES Y RESPONSABILIDADES

La implementación efectiva de la Gobernanza de Datos requiere la participación coordinada de diversos roles y estructuras organizacionales, tanto a nivel regional como local. Cada actor involucrado cumple funciones específicas orientadas a asegurar que los datos sean gestionados, protegidos y utilizados de manera responsable, segura y alineada con los objetivos estratégicos de la Compañía.

Los siguientes roles y responsabilidades establecen el marco base que debe ser aplicado de manera uniforme en todas las operaciones de la región, sin perjuicio de las obligaciones adicionales que pudieran aplicar conforme a la legislación vigente en cada país:

1. **Comité de Compliance:** Órgano colegiado responsable de liderar la gobernanza de datos. Le corresponde:

- Aprobar esta Política y sus actualizaciones.
- Definir lineamientos estratégicos, priorizar iniciativas y resolver conflictos de acceso/uso entre áreas.
- Asegurar coherencia entre esta Política, el MPI y los procedimientos (bases de licitud, retención/eliminación, incidentes, proveedores).
- Revisar periódicamente riesgos asociados al tratamiento de datos y exigir planes de mejora.
- Coordinar con Seguridad de la Información, Cumplimiento y el/los DPO la implementación de controles y evidencias.

2. **Responsable Local de Protección de Datos (rol local aplicado a cada país):**

ECLA designará un responsable local en cada operación para coordinar la correcta implementación de esta Política y del programa de protección de datos a nivel país. Este rol actuará con independencia operativa y contará con acceso a la información, recursos y apoyo necesarios, para lo cual le corresponde:

- Conocer, monitorear y asesorar sobre la legislación, regulación y lineamientos aplicables en materia de protección de datos personales en su jurisdicción, manteniéndose actualizado respecto de cambios normativos, criterios regulatorios y mejores prácticas. Asimismo, deberá informar oportunamente a las áreas operativas correspondientes y al equipo regional de Cumplimiento sobre aquellos cambios o requerimientos locales que puedan impactar el tratamiento de datos personales, brindando apoyo en la implementación de medidas, controles y procesos necesarios para asegurar el cumplimiento de las obligaciones legales y de las políticas corporativas.
- Supervisar el cumplimiento de esta Política, del MPI y de los procedimientos asociados (bases de licitud, retención, incidentes, gestión de terceros), identificando brechas y proponiendo medidas correctivas.
- Validar y mantener la documentación de cumplimiento (registros, evidencias, matrices, instructivos), y apoyar la elaboración de evaluaciones de impacto cuando proceda.
- Coordinar y gestionar el procedimiento de ejercicio de derechos de titulares, incluyendo recepción, análisis, respuesta y registro de solicitudes.

- Coordinar, junto con Seguridad de la Información y Cumplimiento, la gestión de incidentes y brechas que afecten datos personales, asegurando trazabilidad y evidencia.
- Capacitar y promover formación periódica en protección de datos para los equipos que participan en operaciones de tratamiento.
- Actuar como punto de contacto operativo para consultas internas sobre tratamiento de datos, manteniendo deber de reserva y confidencialidad.

Escalamiento obligatorio: cuando se presenten (i) solicitudes de titulares complejas o sensibles, (ii) procedimientos administrativos de fiscalización, requerimientos de la autoridad, o (iii) controversias relevantes sobre bases de licitud, transferencias, subencargados, incidentes o decisiones de alto riesgo, el DPO Local deberá consultar y coordinar con el DPO Regional, previo a adoptar determinaciones finales o emitir respuestas definitivas, salvo que la urgencia impida dicha coordinación, caso en el cual informará de inmediato al DPO Regional.

3. **Responsable Regional de Gobernanza y Protección de Datos:** Emergent Cold LatAm designará un responsable regional encargado de la supervisión, dirección y gobierno del cumplimiento regional en materia de gobernanza de datos y protección de datos personales. Este rol actuará con independencia operativa para emitir criterios, recomendaciones y reportes, y reportará directamente al Directorio u órgano equivalente establecido por la Compañía. En particular, le corresponde:
 - **Definir lineamientos regionales** en materia de gobernanza de datos, protección de datos personales, gestión de riesgos e integración con las políticas corporativas aplicables, asegurando un enfoque homogéneo en toda la región.
 - **Solicitar y revisar reportes periódicos del responsable local**, incluyendo métricas de cumplimiento, riesgos, incidentes, brechas, auditorías, implementación de controles y cualquier otra evidencia relevante.
 - **Evaluar y pronunciarse sobre materias críticas** elevadas por el responsable Local, tales como fiscalizaciones, incidentes relevantes, evaluaciones de impacto cuando apliquen, tratamiento de riesgos significativos, decisiones sobre proveedores y terceros, o eventos que requieran lineamientos regionales. Asimismo, coordinará con Seguridad de la Información, Tecnología y Cumplimiento para asegurar respuestas unificadas y coherentes con requerimientos regulatorios de la región.
 - **Presentar** reportes periódicos al Directorio u órgano equivalente, informando el estado regional del cumplimiento, los principales riesgos, incidentes, métricas,

brechas, medidas de mitigación y planes de mejora, sin perjuicio de reportes extraordinarios cuando la criticidad del caso lo amerite.

7. INTEGRACIÓN CON EL PROGRAMA DE COMPLIANCE CORPORATIVO.

Estos lineamientos forman parte del Programa Corporativo de Compliance, y se integra con los lineamientos, políticas y procedimientos corporativos vigentes en materia de gobernanza de datos, protección de datos personales, seguridad de la información, ciberseguridad, continuidad operativa y otros instrumentos propios del sistema de control interno de la Compañía.

El cumplimiento de esta Política será considerado dentro de los procesos de identificación, evaluación y mitigación de riesgos, así como en las actividades de auditoría, monitoreo y control que emerjan del marco regional. Cualquier incumplimiento de sus disposiciones podrá dar lugar a medidas correctivas, contractuales o disciplinarias conforme a la normativa interna de Emergent Cold LatAm y a la legislación aplicable en cada jurisdicción.

Las modificaciones o ajustes derivados de cambios normativos, tecnológicos u organizacionales deberán ser incorporados oportunamente, y las versiones actualizadas se comunicarán a las áreas responsables y se integrarán en los documentos y procedimientos complementarios que correspondan.

8. VIGENCIA Y REVISIÓN

La presente Política entrará en vigor a partir de su aprobación por el Comité de Compliance de Emergent Cold LatAm, y permanecerá vigente hasta que dicho Comité determine su actualización o reemplazo.

El Comité de Compliance realizará una **revisión periódica**, al menos cada dos años, o con mayor frecuencia cuando se produzcan cambios normativos, tecnológicos, estratégicos u operativos que lo justifiquen. Esta revisión considerará la evolución del marco regulatorio en los países donde opera la Compañía, las prácticas corporativas emergentes, los riesgos asociados al tratamiento de datos y los resultados obtenidos en auditorías o actividades de monitoreo.

Las actualizaciones de esta Política serán comunicadas a todas las áreas involucradas y deberán reflejarse en los procedimientos, lineamientos y documentos complementarios aplicables.